CLAIM AMENDMENTS

This listing of the claims will replace all prior versions, and listing, of claims in the application or previous response to office action:

Listing of Claims

1. (**Currently Amended**) A method for secure communication comprising:

receiving a first profile from a first entity, the first profile indicating electronic commerce information, including a first document exchange protocol, pertaining to the first entity;

receiving a second profile from a second entity, the second profile indicating electronic commerce information, including a second document exchange protocol, pertaining to the second entity;

automatically generating an agreement based on the first profile and the second profile, wherein the agreement includes information pertaining to electronic commerce transactions between the first and second entities;

generating ~~a plurality of~~ **a first** virtual private ~~proxies~~ **proxy and a second virtual private proxy** ~~based on an agreement between a first entity and a second entity~~;

~~associating a~~ **establishing a first secure connection between the** first virtual private proxy ~~of the plurality of virtual private proxies with the first entity~~ **and the first entity** and ~~a~~ **establishing a second secure connection between the** second virtual private proxy ~~of the plurality of virtual private proxies with~~ **and** the second entity;

establishing a logical connection between the first virtual private proxy and the second virtual private proxy;

monitoring data at **at least one of** the first virtual private proxy ~~associated with the first entity~~ **and the second virtual private proxy**;

determining whether ~~the~~ **monitored** data violates the agreement; and

disallowing communication of the **monitored** data ~~from~~ **between** the first virtual private proxy ~~to~~ **and** the second virtual private proxy when the data violates the agreement.

2. (Previously Presented) The method for secure communication according to Claim 1, wherein determining whether the data violates the agreement comprises:

determining whether the data includes a security violation.

3. (**Currently Amended**) The method for secure communication according to Claim 2, wherein the security violation is **selected from the group consisting of:** a virus**, ~~or~~ a** malicious program**, and an intrusion attempt**.

4. (**Currently Amended**) The method for secure communication according to Claim 2, wherein **~~the security violation is an intrusion attempt~~ establishing the first secure connection includes establishing a secure connection with a private session manager of the first entity wherein said private session manager excludes all other remote connections to the first entity**.

5. (Previously Presented) The method for secure communication according to Claim 1, further comprising:

hiding the existence of at least one of the first virtual private proxy or the second virtual private proxy to entities other than the first entity and the second entity of the agreement.

6-7. (Cancelled)

8. (**Currently Amended**) The method for secure communication according to Claim 1, wherein the agreement **~~comprises~~ indicates allowable** types of data **~~allowed~~**.

9. (**Currently Amended**) The method for secure communication according to Claim 8, wherein the agreement further **~~comprises~~ indicates** a transport protocol **~~indication~~** and a transport security protocol **~~indication and wherein the type of data allowed comprises XML~~**

~~data~~.

10. (**Currently Amended**) The method for secure communication according to Claim 9, wherein the agreement further ~~comprises~~ **indicates** ~~a document exchange protocol indication and a~~ process specification ~~document indication~~ **information**.

11-13. (Cancelled)

14. (**Currently Amended**) A system for secure communication comprising:

logic stored on a medium and configured to:

receive a first profile from a first entity, the first profile indicating electronic commerce information, including a first document exchange protocol, pertaining to the first entity;

receive a second profile from a second entity, the second profile indicating electronic commerce information, including a second document exchange protocol, pertaining to the second entity;

automatically generate an agreement based on the first profile and the second profile, wherein the agreement includes information pertaining to electronic commerce transactions between the first and second entities;

generate ~~a plurality of~~ **a first** virtual private ~~proxies~~ **proxy and a second virtual private proxy** ~~based on an agreement between a first entity and a second entity~~;

~~associate~~ **establish** a **first secure communication between the** first virtual private proxy ~~of the plurality of virtual private proxies with the first entity~~ **and the first entity** and ~~a~~ **establish a second secure connection between the** second virtual private proxy ~~of the plurality of virtual private proxies with~~ **and** the second entity;

establish a logical connection between the first virtual private proxy and the second virtual private proxy;

monitor data at **at least one of** the first virtual private proxy ~~associated with the first entity~~ **and the second virtual private proxy**;

determine whether the data violates the agreement; and

disallow communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

15-20. (Cancelled)

21. (**Cancelled**)

22. (**Currently Amended**) The system for secure communication according to Claim ~~21~~ **14**, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication ~~and wherein the type of data allowed comprises XML data~~.

23. (**Currently Amended**) The system for secure communication according to Claim 22, wherein the agreement ~~further comprises~~ **indicates** a document exchange protocol indication and ~~a~~ process specification ~~document indication~~ **information**.

24. (Previously Presented) The system for secure communication according to Claim 14, wherein the logic in determining whether the data violates the agreement determines whether the data includes an intrusion attempt.

25. (Previously Presented) The system for secure communication according to Claim 14, wherein the logic in determining whether the data violates the agreement determines whether the data includes a virus or malicious program.

26-73. (**Cancelled**)

74. (**New**). A non-transitory computer readable medium, including a computer program, executable by a processor, for:

receiving a first profile from a first entity, the first profile indicating electronic

commerce information, including a first document exchange protocol, pertaining to the first entity;

receiving a second profile from a second entity, the second profile indicating electronic commerce information, including a second document exchange protocol, pertaining to the second entity;

automatically generating an agreement based on the first profile and the second profile, wherein the agreement includes information pertaining to electronic commerce transactions between the first and second entities;

generating a first virtual private proxy and a second virtual private proxy;

establishing a first secure connection between the first virtual private proxy and the first entity and establishing a second secure connection between the second virtual private proxy and the second entity;

establishing a logical connection between the first virtual private proxy and the second virtual private proxy;

monitoring data at at least one of the first virtual private proxy and the second virtual private proxy;

determining whether monitored data violates the agreement; and

disallowing communication of the monitored data between the first virtual private proxy and the second virtual private proxy when the data violates the agreement.

75. (**New**). The computer readable medium of claim 74, wherein the document exchange protocol comprises an electronic data interchange (EDI) compliant protocol.

76. (**New**). The computer readable medium of claim 74, wherein the first virtual private proxy comprises a logical access point at a secure switch to the first secure connection and wherein the second virtual private proxy comprises a logical access point at the secure switch to the second secure connection.

77. (**New**). The computer readable medium of claim 74, wherein the first virtual

private proxy comprises a logical representation of a hard-wired access point at a secure switch for a fiber optic connection between the secure switch and the first entity.

78. (**New**). The computer readable medium of claim 74, wherein the agreement further indicates process specification information indicative of businesses processes of at least one of the first entity and the second entity.

79. (**New**). The computer readable medium of claim 78, wherein the process specific information indicates roles, message payloads, message sequence, and operation signals supported by the business processes.